**Amendments to the Specification:**

Please replace the title of the invention with the following amended title:

~~DATA STORAGE CONTROLLER~~ DATA BACKUP IN PRESENCE OF PENDING HAZARD

Please replace the paragraph at page 1, lines 8-9 with the following amended paragraph:

This application is a continuation of U.S. Patent Application No. 09/616,829, filed July 14, 2000 (now U.S. Patent No. 6,684,306), which claims priority from Japanese Patent Application Reference No. 11-356970, filed December 16, 1999, the disclosures of which are incorporated herein by reference.

Please replace the paragraph at page 2, lines 4-11 with the following amended paragraph:

In a representative embodiment according to the present invention, a data storage apparatus is provided. The data storage apparatus can comprise one or more storage media; a cache memory; and a controller. The controller can move data into and out of the storage media and the cache memory. The controller can also receive data from an external source for storage, for example. Further, the data storage apparatus can comprise a hazard sensor. Responsive to the hazard sensor detecting a probable occurrence of a hazardous event, the controller can copy data from the cache memory to the storage media in order to preserve a copy of the data.

Please replace the paragraph at page 3, lines 1-12 with the following amended paragraph:

In a still yet further representative embodiment according to the present invention, a data storage controller can prioritize the data storage to a local non-volatile disk. This can be especially useful in installations where the remote copying is used to create the remote data merely as a backup data. In such embodiments, remote copying provides a non-stop data backup, while the backup to the other media such as magnetic tape, for example, requires stopping of the operation of the system. Thus, in case of a serious disaster, it [[is]] may be important to store the data at the local site[[.]] ([[To]] to a non-volatile disk, for example). Another embodiment in which higher priority may be given to local copying are

installations where there is a possibility that the remote copying path could also break down. In such installations, it is of little use to copy the data to the remote site. Thus, in such embodiments, storing the data at the local site, to a non-volatile disk, or the like, will be given a higher priority over making a remote copy of the data.

Please replace the paragraph at page 5, lines 5-17 with the following amended paragraph:

The present invention provides techniques for performing real time backup of data in the presence of a pending hazard, such as a natural disaster, or the like. Embodiments can provide data storage controllers, networked data storage systems, methods and the like, that detect imminent hazardous conditions and alter backup behavior to provide greater integrity of backed up data. In a specific embodiment, a system that updates data to a backup device after updating an original copy of the data, is provided. The system can include a recognition part, such as a device that detects a probable occurrence of a hazardous event. The detection device can comprise a sensor within the storage controller, for example. Sensors can include an earthquake sensor, a fire sensor, a smoke sensor, a moisture sensor, a flood sensor, a thunderstorm sensor or a supply voltage sensor. In specific embodiments, the detection device can comprise, for example, a receiver that receives the relevant information relating to the probable occurrence of a hazardous event from an external device or that receives a warning signal from an external device.

Please replace the paragraph at page 5, line 29 to page 6, line 3 with the following amended paragraph:

A variety of techniques may be used in making backup copies of data in storage. In a technique used in conjunction with a synchronous remote copy technology, the operation of a primary system is continued by updating only the primary data. Then, a remote copy that updates the secondary data asynchronously is performed by arranging a secondary processing device for updating the secondary data separated from the primary processing device for operating the primary system. [[For a]] A more detailed description of such techniques[[, further reference]] may be [[had to a]] found in Japanese patent unexamined publication 07-239799, for example.

Please replace the paragraph at page 6, lines 4-9 with the following amended paragraph:

In another technique, an asynchronous remote copy is performed by a primary storage controller to record primary data. Asynchronous copying is also performed by a secondary storage controller in order to record secondary data in the storage controller to control actual data recording to a recording media. Further [[reference]] details may be [[had to a]] found in Japanese patent unexamined publication 11-85408, for more details regarding such techniques.

Please replace the paragraph at page 6, lines 10-20 with the following amended paragraph:

A variety of techniques can be used to recognize the extent to which secondary data has been updated with respect to the primary data. For instance, an index that indicates an order representing the order of various portions of the primary data to be stored can be also transferred to the primary storage controller when an update of data is requested from the primary processing device. Subsequently, this index can then be transferred to the secondary processing device or the secondary storage controller. Such an index can provide a clear indication of the extent to which the secondary data has been updated. The index can indicate an order with respect to the secondary processing device or the secondary storage controller, so that the various portions of the data are stored in the proper order. Further, this index can be recorded to a journal file, or the like, in which the progress of the primary system processing is recorded. By obtaining such indications, it is possible to reproduce the lost data or to retry the processing, for example.

Please replace the paragraph at page 6, line 21 to page 7, line 4 with the following amended paragraph:

Fig. 1A illustrates a diagram showing a representative storage system for performing a remote dual copy in a general-purpose computer system in a representative embodiment of the present invention. In a representative embodiment according to the present invention illustrated by Fig. 1A, a storage system comprises a Host CPU 10, which is a central processing unit in a host unit, a primary disk controller 20, and a primary disk device 30, and constitute [[that comprise]] the primary storage system. Fig. 1A further illustrates a secondary disk controller 21 and a secondary disk device 31 of the secondary

storage system, which is a destination for copying backup data. The primary disk controller 20 comprises a data copy control part 201 which can be circuitry, program logic, or a combination thereof, that controls copying data to the secondary system[,]; a memory such as a data buffer 202 that holds the copy data temporarily[,]; and a recognition part 203 that recognizes a hazard of losing the held data. The recognition part may comprise a detection device, such as a sensor within the primary storage controller 20, such as an earthquake sensor, a thermal sensor to detect a fire, a smoke sensor, a thunder sensor, a moisture sensor, a flood sensor or a detector of supply voltage hazard which may cause a system outage. The memory may be a cache memory 204 as shown in Fig. 1B, for example.

Please replace the paragraph at page 7, line 25 to page 8, line 6 with the following amended paragraph:

In specific embodiments, recognition part 203 can comprise a variety of sensors, or other hazard detection devices. For example, a sensor provided within the primary disk controller 20 itself may be used. The sensor may be a seismograph to detect an earthquake, for example, or a thermometer or a smoke sensor to detect a fire. A [[lightening]] lightning/thunder or storm sensor, could be used to detect inclement weather. A voltage/current detector can be used to detect electric fluctuations. A moisture sensor and/or a flood sensor could be used to detect the presence of water. Thus, recognition part 203 can comprise many types of sensors, or other devices, can be used to detect a probable occurrence of a hazard that could cause damage to the primary disk controller 20 or the primary disk device 30. For example, in specific embodiments, a receiving device that receives information from a sensor located in a room or a building where the primary system is placed may be used. The recognition part 203 may also comprise a recognition system that receives an external attention/warning information or public information broadcast by an external organization such as a meteorological agency, National Weather Service or the like.

Please replace the paragraph at page 8, line 29 to page 9, line 8 with the following amended paragraph:

In another representative embodiment according to the present invention, a data storage controller, such as primary data storage controller 20 of Fig. 1A, for example, can prioritize the data storage to a local non-volatile disk. This can be especially useful in

installations where the remote copying is used to create the remote data merely as [[a]] backup data. In such embodiments, remote copying provides a non-stop data backup, while the backup to the other media such as magnetic tape, for example, requires stopping of the operation of the system. Thus, in case of a disaster, it may be important to store the data at the local site[[.]] ([[To]] to a non-volatile disk, for example). Another embodiment in which higher priority may be given to local copying are installations where there is a possibility that the remote copying path could also break down. In such installations, it is of little use to copy the data to the remote site. Thus, in such embodiments, storing the data at the local site, to a non-volatile disk, or the like, will be given a higher priority over making a remote copy of the data.

Please replace the paragraph at page 9, lines 9-25 with the following amended paragraph:

Fig. 2A illustrates a diagram of a representative configuration of a stand alone disk storage system with a hazard sensor in accordance with a representative embodiment of the present invention. Fig. 2A illustrates a disk controller 220 in a particular embodiment. Disk controller 220 comprises a cache memory 204, operable to provide temporary storage for information received from a Host CPU 10, through a channel adapter (CHA) 701, for example. Further, disk controller 220 comprises a plurality of disk storage units, including a disk storage 30, connected to disk controller 220 through a disk adapter (DKA) 702, for example. The disk storage unit 30 provides persistent storage for information written to the disk from Host CPU 10, for example, for later retrieval. Disk controller 220 can further comprise a recognition part 203, which can comprise a detection device, such as a sensor, for example, that can be an earthquake sensor, a thermal sensor to detect a fire, a smoke sensor, a moisture sensor, a flood sensor, a thunder/lightening sensor or a detector of supply voltage hazard which may cause a system outage. A bus 703 interconnects the channel adapter 701, cache memory 204, disk adapter 702 and recognition part 203. Disk controller 220 can further comprise other and varied elements, not shown here, without departing from the scope of the present invention.

Please replace the paragraph at page 9, line 26 to page 10, line 3 with the following amended paragraph:

Fig. 2B illustrates a diagram of a representative operation of a stand alone disk storage system with a hazard sensor in accordance with a representative embodiment of the present invention. Fig. 2B illustrates processing in a stand alone [[storage system]] disk controller 220 of Fig. 2A, for example, when no hazard is present. Write requests (1) made by a Host CPU 10 are received by disk controller 220. Responsive to the write requests, disk controller [[250]] 220 stores write data in cache memory 204. When the write data has been stored in cache memory 204, a write completion (2) is sent to host CPU 10 in indicate that the data has been successfully received at the disk controller 220. The Host CPU 10, upon receipt of the completion message, will continue processing the job that made the write data request. Then, the write data is transferred (3) from the cache memory 204 into disk storage 30, for example.

Please replace the paragraph at page 10, lines 4-14 with the following amended paragraph:

Fig. 2C illustrates a diagram of a representative operation of a stand alone disk storage system with a hazard sensor in accordance with a representative embodiment of the present invention. Fig. 2C illustrates processing in a stand alone [[storage system]] disk controller 220 of Fig. 2A, for example, when a hazard has been detected. Write requests (1) made by a Host CPU 10 are received by disk controller 220. Responsive to the write requests, disk controller 220 stores write data in cache memory 204. Then, the write data is transferred (2) from the cache memory 204 into disk storage 30, for example. When the write data has been stored in cache memory 204, a write completion (3) is sent to host CPU 10 to indicate that the data has been successfully received at the disk controller 220. The Host CPU 10, upon receipt of the completion message, will continue processing the job that made the write data request.

Please replace the paragraph at page 10, lines 22-27 with the following amended paragraph:

Another representative embodiment according to the present invention will be explained by referring to Fig. 3A. Fig. 3A illustrates a system according to a representative embodiment, comprising a secondary disk controller 21 that is provided with a cache memory

214 and an asynchronous/synchronous switching part 215. Other constructions are substantially similar to those discussed herein above with respect to Fig. 1A and Fig. 1B.

Please replace the paragraph at page 12, line 26 to page 13, line 6 with the following amended paragraph:

Fig. 5 illustrates operation of synchronous remote dual copy in the data copy control part 201 in a representative embodiment according to the present invention. Fig. 5 illustrates a step 502, in which a primary disk controller, such as primary disk controller 20 of Fig. 3A, for example, receives a data write request from Host CPU 10. In a step 504, responsive to the data write request from the Host CPU 10, primary disk controller 20 determines whether there is un-copied data present in cache memory 204. If, in step 504 it is determined that un-copied data remains in the cache memory 204 for the secondary disk device 31 after shifting to synchronous remote dual copy mode, then in a step 508, the data copy control part 201 sets a flag which indicates synchronous remote dual copy operation with un-copied data remaining (that is, a synchronous copy flag with un-copied data remaining = 1). Then, in a step 510, data is transferred with the flag attached in order to provide an indication of temporary holding in synchronous remote dual copy mode. The flag is used to indicate transfer of the data to the secondary disk controller 21 in synchronous remote dual copy mode.

Please replace the paragraph at page 14, line 28 to page 15, line 8 with the following amended paragraph:

In a representative embodiment according to the present invention as illustrated by Fig. 4, a plurality of primary disk controllers may be connected to a single host CPU and further to a single remotable secondary disk controller. Recognition timing of each primary disk controller can be different, since each primary disk controller recognizes the possibility of losing data individually. Recognition timing is the timing of recognizing a probable occurrence of a hazardous event by a primary disk controller. In this embodiment, when the data to be written to the primary disk controller 20 from the Host CPU 10 and the data to be written to the primary disk controller 20' from the Host CPU 10 relate to each other, this relationship is lost if either of the data is the only un-erased data remaining (that is, copied data). Specific embodiments can prevent such occurrence by providing for either of

the primary disk controller 20 and the primary disk controller 20', upon recognizing the possibility of losing data, to notify the other primary disk controller of this possibility. The recognition timing on each side of the possibility of losing data coincides to this notification, so that the damage resulting from a loss of data due to a disaster can be reduced even in case of the configuration of a plurality of primary disk controllers.